REPÚBLICA DE CHILE
I. MUNICIPALIDAD DE CONCON
ADMISTRACIÓN Y FINANZAS

DECRETO N.° 4426

EN CONCÓN, 30 DIC 2024

VISTOS Y TENIENDO PRESENTE:

A. Las facultades que me confieren la Ley N°18.695, Orgánica Constitucional de Municipalidades.
B. Las facultades emanadas de la Ley 19.880, en su artículo 3°.
C. Decreto 83, Ministerio secretaria general de la Presidencia de fecha 12.01.2005.
D. Ordinario 088/2016, de fecha 15 de noviembre de 2016, del Departamento de Control Interno, solicitando conformación "Comité de Seguridad Informática de la Municipalidad".
E. Ordinario 193/2016, de fecha 18 de noviembre de 2016, del Departamento de Administración y Finanzas, invitando al Sr. alcalde a Reunión de Comité.
F. Ordinario 198/2016, de fecha 23 de noviembre de 2016, del Departamento de Administración y Finanzas, informando a la Sra. alcaldesa (S) que no se pudo constituir el Comité.
G. Ordinario 199/2016, de fecha 23 de noviembre de 2016, del Departamento de Administración y Finanzas, citando a los diferentes Departamentos a Reunión de Comité.
H. Ordinario 204/2016, de fecha O1 de diciembre de 2016, del Departamento de Administración y Finanzas, informando a la Sra. alcaldesa (S) sobre 2da. Reunión del Comité.
I. Ordinario 205/2016, de fecha O1 de diciembre de 2016, del Departamento de Administración y Finanzas, citando a los diferentes Departamentos a Reunión de Comité.
J. Ordinario 215/2016, de fecha 13 de diciembre de 2016, del Departamento de Administración y Finanzas, citando a los diferentes Departamentos a Reunión de Comité.
K. Planilla de fecha 16.12.2016 con votación y firmas de Aprobación sobre Manual de Políticas y Estándares de Seguridad Informáticá.
L. Decreto alcaldicio N° 3035 de fecha 30 de diciembre del 2016, el cual aprueba "Manual de Políticas y estándares de Seguridad Informatica"
M. Planilla y acta N3 de fecha 13.12.2024 con votación y firma de aprobación sobre la modificación y actualización de "Manual de Políticas y estándares de seguridad informatica".

DECRETO

1. **APRUEBESE,** Actualización "Manual de Políticas y Estándares de Seguridad Informática" para usuarios de la Municipalidad, Educación y Salud, según acuerdo del Comité de Seguridad Informática de fecha 13 de diciembre de 2024.

27 DIC 2024

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

MUNICIPALIDAD DE CONCON

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

OFICINA DE INFORMATICA

Diciembre 2024

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO
27 DIC 2024

CONTENIDO

Propósito....5

Introducción....5

Objetivo....5

Alcance....5

Justificación....6

Sanciones por incumplimiento....6

Beneficios....6

1.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política....6

1.1. Obligaciones de los usuarios....6

1.2. Acuerdos de uso y confidencialidad....6

1.3. Entrenamiento en seguridad informática....7

1.4. Medidas disciplinarias....7

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política....7

2.1. Resguardo y protección de la información....7

2.2. Controles de acceso físico....8

2.3. Seguridad en áreas de trabajo....9

2.4. Protección y ubicación de los equipos....10

2.5. Mantenimiento de equipo....11

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO
27 DIC 2024

2.6. Pérdida o transferencia de equipo....11
2.7. Uso de dispositivos especiales....12
2.8. Daño del equipo....12

3.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política....13
3.1. Uso de medios de almacenamiento....13
3.2. Instalación de Software....14
3.3. Identificación del incidente....15
3.4. Administración de la configuración....15
3.5. Seguridad de la red....15
3.6. Uso del correo electrónico....16
3.7. Control es contra código malicioso....17
3.8. Permisos de uso de Internet....19

4.-POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESOLÓGICO

Política....20
4.1. Control es de acceso lógico....20
4.2. Administración de privilegios....21
4.3. Equipo desatendido....21
4.4. Administración y uso de contraseñas....22
4.5. Control de accesos remotos....23

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

27 DIC 2024

5.-POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política.....23

5.1. Derechos de propiedad intelectual.....23

5.2. Revisiones del cumplimiento.....24

5.3. Violaciones de Seguridad Informática.....24

GLOSARIO DE TÉRMINOS.....25

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

27 DIC 2024

Propósito

El presente documento tiene como finalidad dar a conocer las Políticas y estándares de Seguridad Informática que deberán observar Los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad de Concon.

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Municipalidad de Concon en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal.
- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Cumplimiento.

Estas Políticas en seguridad informática se encuentran alineadas con el Estándar NCh 2777.Of2003.

Objetivo

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal de la Municipalidad de Concon, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

27 DIC 2024

Alcance

El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo Computacional, aplicaciones y servicios informáticos de la Municipalidad de Concon.

Justificación

La Oficina de informática de la Municipalidad de Concon está facultada para definir Políticas y Estándares en materia informática.

Sanciones por Incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

Las Políticas y Estándares de Seguridad Informática establecidos Dentro de este documento son la base para la protección de los activos tecnológicos e información de la Municipalidad de Concon.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la Municipalidad de Concon, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

1.1. Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios Informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos de la Municipalidad de Concon deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información que posee la Municipalidad de Concon, y cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

1.3. Entrenamiento en Seguridad Informática.

Todo empleado de la Municipalidad de Concon, de nuevo ingreso deberá:

- Leer y firmar el Manual de Políticas y Estándares de Seguridad de la Municipalidad de Concon, donde se dan a conocerlas obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

1.4. Medidas disciplinarias.

Cuando La Oficina de Informática identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Órgano Interno de Control, para los efectos de su competencia y atribuciones.

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Municipalidad de Concon, sólo a personas autorizadas para salvaguarda.

2.1 Resguardo y protección de la información.

2.1.1. El usuario deberá reportar de forma inmediata a la Oficina de Informática, cuando detecte que existan riesgos reales o potenciales para equipos computacionales o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2. El usuario tiene la obligación de proteger las memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

2.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Municipalidad de Concon que se encuentre almacenada en los equipos computacionales personales que tengan asignados.

2.2. Controles de acceso físico.

Cualquier persona que tenga acceso a las instalaciones de la Municipalidad de Concon, deberá portar a la vista una credencial que identifique la calidad en la que se encuentra al interior de las instalaciones, pudiendo ser éstas como funcionario o visita.

Se debe registrar en portería toda persona externa que quiera acceder a dependencias de la Municipalidad de Concon, deberá identificarse e indicar motivo de la visita, posteriormente se deberá constatar con el departamento respectivo y de ser positivo el ingreso se le debe proporcionar una credencial de visita que la identifique como tal.

En el caso del ingreso de equipos computacionales que no sean propiedad de la Municipalidad de Concón, el personal externo deberá demostrar que el o los equipos cuentan con las siguientes especificaciones técnicas para conectarse a la red interna de la institución; estos requisitos son firewall activado, antivirus empresarial activo y con su base de datos actualizada al presente día, sistema operativo más reciente (Windows 10 22h2 – Windows 11 23h2 o superior, Linux kernel 6.4 o superior y macOS bigsur o superior) por otra parte, al ingresar un dispositivo extraíble el personal externo deberá realizar un análisis al dispositivo con su equipo asignado, en caso de no contar con esto último se deberá dar consentimiento para que la unidad de informática realiza el análisis en un entorno controlado.

el jefe de Informática podrá negar la autorización si establece que es potencialmente riesgoso y/o comprometa la red de datos o la seguridad.

Todo acceso físico a las personas será restringido, debiéndose gestionar y documentar.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

El proceso para la obtención de las credenciales, tarjetas de acceso magnético o claves de acceso a instalaciones de la Municipalidad de Concon deberán ser solicitadas por el jefe de departamento al cual pertenece o desempeña labores el funcionario y deberá incluir la aprobación del encargado de la Oficina de informática de la Municipalidad de Concon. La emisión de las credenciales, tarjetas de acceso magnético o claves de acceso será efectuada únicamente por la Oficina de informática de la Municipalidad de Concon, entidad que llevará el registro de las emisiones.

Las tarjetas de acceso magnético o claves de acceso NO deben ser compartidas o cedidas a otros.

Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos a la Oficina de Informática de la Municipalidad de Concon. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.

La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados a la Oficina de Informática de la Municipalidad de Concon al correo informatica@concon.cl, incluyendo en el mensaje los siguientes datos: RUT, Nombre completo del funcionario, dependencia, y circunstancias en las cuales sucedió el robo o pérdida.

2.3. Seguridad en áreas de trabajo.

Los Centros de Cómputo de la Municipalidad de Concon son áreas restringidas, por lo que sólo el personal autorizado por la Oficina de Informática puede acceder a ellos.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

2.4. Protección y ubicación de los equipos.

2.4.1. Los usuarios no deben mover o reubicar los equipos computacionales o de telecomunicaciones, instalar o desinstalar dispositivos ni software, tampoco se pueden retirar sellos de los mismos sin la autorización del Encargado de Informática, debiéndose solicitar al mismo, en caso de requerir este servicio.

2.4.2. El Encargado de Bodega e Inventario será el responsable de generar el resguardo y recabar la firma del usuario como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Departamento.

2.4.3. Los equipos computacionales asignado, deberán ser para uso exclusivo de las funciones asignadas al usuario de la Municipalidad de Concon.

2.4.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.6. Mientras se opera el equipo computacional, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.

2.4.7. No se pueden colocar objetos encima del equipo o cubrirlos orificios de ventilación del monitor o del gabinete.

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

2.4.9. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.4.10. Cuando se requiera realizar cambios múltiples de equipos computacionales o reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Oficina de Informática y al Encargado de Bodega e Inventario, a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.4.11. Queda prohibido que el usuario abra o desarme los equipos computacionales, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.5. Mantenimiento de equipo.

2.5.1. Únicamente el personal autorizado de la Oficina de Informática podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación el funcionario deberá indicar a informática cuál es la información sensible que se encuentre en el equipo para así evitar pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal del departamento de informática para respaldos.

2.6. Pérdida o transferencia de equipo.

2.6.1. El usuario que tenga bajo su resguardo algún equipo Computacional será responsable de su uso y custodia, en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

2.6.2. El resguardo para los Laptops o Notebook, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3. El usuario deberá dar aviso de inmediato al Encargado de Informática y al Encargado de Bodega e Inventario de la desaparición, robo o extravío del equipo computacional o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales.

2.7.1 . El uso de pendrives, discos duros externos, memorias SD, u otro dispositivo de almacenamiento masivo externo, es de uso exclusivo para respaldos de información, que por su volumen así lo justifiquen, queda estrictamente prohibido que éstos dispositivos salgan de la Municipalidad de Concón ya que esta información perteneciente a la institución y es creada con recursos estatales.
Los dispositivos externos deben ser guardados bajo llave por la directiva o jefaturas de los departamentos y con el resguardo correspondiente, tratándose de información sensible o privilegiada.

2.7.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

2.7.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.7.4. Los módems internos deberán existir solo en las computadoras portátiles y NO se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice el Encargado de Informática.

2.8. Daño del equipo.

El equipo computacional o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.- POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán utilizar los mecanismos institucionales para protegerla información que reside y utiliza la infraestructura de la Municipalidad de Concon. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de Municipalidad de Concon, o hacia redes externas como internet.

Los usuarios de la Municipalidad de Concon que hagan uso de equipo computacionales, deben conocer y aplicarlas medidas para la prevención de código malicioso como pueden ser virus, *malware* o *spyware*. El usuario puede acudir al Encargado de Informática, o a su jefe inmediato, para que éste solicite asesoría.

3.1. Uso de medios de almacenamiento

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de Información compartido, deberá contar con la autorización del Encargado de Informática, jefe inmediato del usuario y del titular del área dueña de la información.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con timbre y firma del titular del área.

3.1.2. Los funcionarios deben mantener la información sensible y confidencial en una carpeta especifica la cual debe tener la inicial de su nombre acompañado del apellido esto último para que la unidad informática pueda respaldar eficientemente, este respaldo será guardado periódicamente en un servidor ftp (FILE TRANSFER PROTOCOL) Y solo los equipos que contengan información sensible y/o privilegiada según lo determine la unidad de informática y directores(as), quedando excepta cualquier información personal del funcionario Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría al Encargado de Informática, para que dichos asesores determinen el medio en que se realizará dicho respaldo.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.1.3. En caso de que por el volumen de información se requiera algún respaldo en disco duro, este servicio deberá solicitarse por escrito al jefe de Informática, y deberá contar con la firma del titular del área.

3.1.4. Los trabajadores de la Municipalidad de Concón deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Encargado de Informática, en términos que indica la Ley 19628, demás criterios y procedimientos establecidos en esta materia.

3.1.5. Las actividades que realicen los usuarios de la Municipalidad de Concon en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.2. Instalación de Software.

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad de la Municipalidad de Concon, deberán justificar su uso y solicitar su autorización al Encargado de Informática, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo computacionales donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.
Si el dueño del software no presenta la factura de compra del software, el personal asignado por el Encargado de Informática procederá de manera inmediata a desinstalar dicho Software.

3.2.2. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa *(software)* en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Municipalidad de Concon, que no esté autorizado por el Encargado de Informática.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.3. Identificación del incidente.

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Encargado de Informática o a su jefatura inmediata, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, la unidad informática deberá notificar al titular de su departamento.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Municipalidad de Concón, debe ser reportado al Encargado de Informática.

3.4. Administración de la configuración.

Los usuarios de las áreas de la Municipalidad de Concón no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos computacionales utilizando el protocolo de transferencia de archivos, empleando la infraestructura de red de la Municipalidad de Concón, sin la autorización por escrito del Encargado de Informática. Para estos efectos el Encargado de Informática dispondrá de un servicio FTP al cual los usuarios de la Municipalidad de Concón podrán acceder mediante usuario y password, que le serán proporcionados oportunamente.

3.5. Seguridad de la red.

Será considerado como un ataque a la seguridad informática y una Falta grave, cualquier actividad no autorizada por el Encargado de Informática, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la Municipalidad de Concón, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.6. Uso del correo electrónico.

3.6.1. Los usuarios no deben usar cuentas de correo electrónico propias, en El desempeño de sus funciones, el Encargado de Informática proporcionará cuentas de correo institucionales a los usuarios de la Municipalidad de Concón, en las cuales su contenido es de propiedad de la Municipalidad de Concón y se encuentran protegidas por la actual normativa vigente. Se debe incluir en todos los correos enviados, el pie de firma estándar e incluir la nota "La información contenida en este correo electrónico, así como en cualquiera de sus adjuntos, es confidencial y está dirigida exclusivamente a él o los destinatarios indicados. Cualquier uso, reproducción, divulgación o distribución por otras personas distintas a él, o los destinatarios, está estrictamente prohibida. Si ha recibido este correo por error, por favor notifíquelo inmediatamente al remitente y bórrelo de su sistema sin dejar copia del mismo. (Los acentos han sido suprimidos intencionalmente para no exponer al texto a reemplazos de los caracteres acentuados)".
Los usuarios no deben usar cuentas asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien Más (mientras esta persona se encuentra fuera o ausente), el usuario Ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Municipalidad de Concón, a menos que cuente con la autorización del titular del área.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Municipalidad de Concón. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el Encargado de Informática.

3.6.4. La Municipalidad de Concon, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

De personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la Municipalidad de Concon o realizado acciones no autorizadas. Como la información del correo electrónico institucional de la Municipalidad de Concon es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.6.5. El usuario debe de utilizar el correo electrónico de la Municipalidad de Concon, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.6. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso.

3.7.1. Para prevenir infecciones por virus informáticos, los usuarios de la Municipalidad de Concon, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y Validado por el Encargado de Informática.

3.7.2.Los usuarios de la Municipalidad de Concon, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos externos, pendrives, CD´s, DVD's estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Encargado de Informática.

3.7.3. El usuario debe verificar mediante el software de antivirus autorizado por el Encargado de Informática que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

3.7.4. Ningún usuario de la Municipalidad de Concon debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la Municipalidad de Concon. El incumplimiento de este estándar será considerado una falta grave.

3.7.5. Ningún usuario ni empleado de la Municipalidad de Concon, o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Encargado de Informática.

3.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Encargado de Informática para la detección y erradicación del virus.

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo Computacional personal portátil, será responsable de solicitar de manera periódica al Encargado de Informática las actualizaciones del software de antivirus.

3.7.8. Los usuarios NO deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Encargado de Informática en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;
- Navegadores; u
- Otros programas.

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario de la Municipalidad de Concon debe intentar erradicarlos de las computadoras, lo indicado es llamar al Encargado de Informática para que sean ellos quienes lo solucionen.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.8. Permisos de uso de Internet.

3.8.1. El acceso a internet provisto a los usuarios de la Municipalidad de Concon es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de Control de la Municipalidad de Concon.

3.8.2. La asignación del servicio de internet, deberá solicitarse por Escrito al Encargado de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno Del titular del área correspondiente.

3.8.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Municipalidad de Concon.

3.8.4. Los usuarios con acceso a Internet la Municipalidad de Concon tienen que reportar todos los incidentes de seguridad informática al Encargado de Informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.5. El acceso y uso de módem en la Municipalidad de Concon tiene que ser previamente autorizado por el Encargado de Informática.

3.8.7. Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos al monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de *software* sin la autorización del Encargado de Informática.
- La utilización de internet es para el desempeño de su función y puesto en la Municipalidad de Concon y no para propósitos Personales.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

3.8.8. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea serán administrados por el Encargado de Informática de acuerdo a las necesidades particulares de los usuarios según la labor que desempeña, por lo que los accesos a paginas restringidas deberán ser solicitados mediante formulario escrito, deberá ser firmado y timbrado por el jefe de la unidad a cargo autorizando dichos accesos.

4.- POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESOS LÓGICOS

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (*user ID)* y contraseña (*password*), necesarios para acceder a la información y a la infraestructura tecnológica de la Municipalidad de Concon, por lo cual deberá mantenerlo de forma confidencial.

Sólo el Alcalde de la Municipalidad de Concon, puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la Municipalidad de Concon, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

4.1. Controles de acceso lógico.

4.1.1. El acceso a la infraestructura tecnológica de la Municipalidad de Concon para personal externo debe ser autorizado por el Encargado de Informática.

4.1.2. Está prohibido que los usuarios utilicen la infraestructura Tecnológica de la Municipalidad de Concon para obtener acceso no autorizado a la información u otros sistemas de información de la Municipalidad de Concon.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Encargado de Informática antes de poder usar la infraestructura tecnológica de la Municipalidad de Concon.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Municipalidad de Concon , a menos que se tenga autorización del Encargado de Informática.

4.1.6. Cada usuario que accede a la infraestructura tecnológica de la Municipalidad de Concon, debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de los usuarios.

4.2.1. Cualquier cambio en los roles y responsabilidades de privilegios que modifique sus privilegios de acceso a la infraestructura tecnológica la Municipalidad de Concon, deberán ser notificados por escrito o vía correo electrónico al Encargado de Informática, con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido.

Los usuarios deberán mantener sus equipos Computacionales con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por el Encargado de Informática), como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

4.4. Administración y uso de contraseñas.

4.4.1. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al Encargado de Informática, indicando si es de acceso a la red o a módulos de sistemas, para que se le bloqueen los accesos y se proporcione una nueva contraseña.

4.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el Encargado de Informática como empleado de la Municipalidad de Concon.

4.4.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.4.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10).Estos caracteres deben ser alfanuméricos, o sea, números y letras;

- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.

- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.7. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

4.4.8. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

4.4.9. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.4.10. Los cambios o desbloqueo de contraseñas solicitados por el usuario al Encargado de Informática serán solicitados mediante solicitud o e-mail, firmado por el jefe inmediato del usuario que lo requiere.

4.4.11. El departamento de gestión deberá dar aviso a la brevedad al Departamento de informatica de la Desvinculación de funcionarios y/o cambios de los mismos a otras dependencias, con la finalidad de que personal de informatica pueda realizar la eliminación de cuentas de correo, eliminación usuarios de programas de gestión interna y respaldo de información del o los equipo utilizados por el funcionario.

programas de gestión interna y respaldo de información

4.5. Control de accesos remotos

4.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del Encargado de Informática.

4.5.2. La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el Encargado de Informática.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA.

Política

De acuerdo al Decreto N° 83 del año 2005, del ministerio secretaría general De la presidencia de la república de Chile que "Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos".

5.1. Derechos de Propiedad Intelectual.

5.1.1. Está prohibido por las leyes de derechos de autor y por la Municipalidad de Concon, realizar copia no autorizadas de

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

Software, ya sea adquirido o desarrollado por la Municipalidad de Concon.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la Oficina de Informática, o sea coordinado por éste, son propiedad intelectual de la Municipalidad de Concon.

5.2. Revisiones del cumplimiento

5.2.1. El Encargado de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

5.2.2. El Encargado de Informática, podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática.

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Encargado de Informática.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.
Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Encargado de Informática.

5.3.3. Ningún usuario de la Municipalidad de Concon debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Encargado de Informática.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para auto replicarse, dañar, afectar el desempeño, acceso a

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

las computadoras, redes e información de la Municipalidad de Concon.

Para los efectos del presente manual, se escribe el presente glosario de términos:

GLOSARIODE TÉRMINOS

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Es el privilegio de una persona para utilizar un objeto o infraestructura.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
(B)	
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
(C)	
Confidencialidad	Se refiere a la obligación de los servidores a no divulgar.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

	Información a personal no autorizado para su conocimiento.
Contraseña Password	Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salva guardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas .Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.
(D)	
Disponibilidad	Se refiere a que la información esté disponible en el momento que se necesite.
(E)	
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
(F)	
Falta administrativa	Acción u omisión contemplada por la normatividad aplicable a la actividad de un funcionario de la Municipalidad de Concon, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.
FTP	Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporción a un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
(G)	
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
(H)	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
(I)	

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

Identificador de Usuario	Nombre de usuario (también referido como User ID) único asignado a un servidor para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad	Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (worldwideweb) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo.
(M)	
Maltrato	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la Municipalidad de Concon. Se contemplan dentro de éste al descuido y la negligencia.
Malware	Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, *spyware*, *troyanos*, *rootkits*, *backdoors*, *adware* y gusanos.
Mecanismos de seguridad o de	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. Que se utiliza para disminuir
control	La probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamiento magnéticos	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.
(N)	

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

"Necesidad de saber" principio	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidad es dentro de la Comisión.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
(P)	
Password	Véase Contraseña.
(R)	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.
(S)	
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

	Proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Spyware	Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.
(U)	
UserID	Véase Identificador de Usuario.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
(V)	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

I. MUNICIPALIDAD DE CONCON
DIRECTOR
CONTROL INTERNO

2. **DÉJESE**, sin efecto "Manual de Políticas y Estándares de Seguridad Informática" aprobado en Decreto Alcaldicio N°3035 de fecha 30 de diciembre del 2016.

3. **NOTIFIQUESE**, por secretaria Municipal.

NÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE.

I. MUNICIPALIDAD DE CONCON SECRETARIA MUNICIPAL

MARIA LILIANA ESPINOZA GODOY
SECRETARIO MUNICIPAL

I. MUNICIPALIDAD DE CONCON ALCALDE

FREDDY RAMIREZ VILLALOBOS
ALCALDE

FRV/MLEG/EAO/pmr
Distribución:
1.- Alcaldia
2.- Secretaria Municipal.
3.- Control
4.- Salud
5.- Informático Salud (SR. Gonzalo Román)
6.- Educación
7.-jefe Transparencia
8.- Archivo Daf

I. MUNICIPALIDAD DE CONCON		
Dirección de Control		
Objetado	Observado	Revisado 27 DIC 2024

27 DIC 2024

I. MUNICIPALIDAD DE CONCON DIRECTOR CONTROL INTERNO